IAPQR Transactions
ISSN **0970-0102** ; Vol. 50, Issue 01, No. 01 : 2025

DIGITAL FORENSICS

Ms.T.Nithya, ASSISTANT PROFESSOR, PG DEPARTMENT OF COMPUTER APPLICATIONS
MARUDHAR KESARI JAIN COLLEGE FOR WOMEN (AUTONOMOUS), VANIYAMBADI

ABSTRACT

s the world is growing towards digitalization, all these industries are utilizing the benefits of digitalization in the working process. With the help of digitalization, the working procedures are performing very fast and effectively. To use digitalization we just need a computer or a system. Some forensics software tools are there that need to be installed in the computers so one can perform the task. It gives us the benefit of fast operations. For example in the year 2020, the computers are too much helpful for the Covid-19 positive forensics test. Only with the help of computers, it is too much easier to test.

Keywords- Computer, Digital world, Forensic world

INTRODUCTION

Digital Forensics is the form of using the knowledge of science and the latest technology and that can be used by the court of law. The main aim of digital forensics is to present a structured inspection while arranging a documented series of proof and evidence to find out completely what happened on a digital device. It is the great evolution of technology; the devices for digital forensics must be updated. Forensics is depended on the of that every criminal leaves a mark of him behind-when two things linked to each other, then transferred between them, and one criminal can be linked to the crime through marks evidence conveyed from the scene of the crime

HISTORY:

- (1847-1915) Hans Gross, the first person uses the technical study for criminal inquiry purposes. Since 1990, what we known as digital forensics was generally termed 'computer forensics'.
- In 1932,the FBI builds a laboratory to provide the facility of forensics to the agents. .The main motive of the event is called the International Law Enforcement Conference on Computer Evidence.
- In 1978, the digital offense was first investigated in the Florida Computer Crime Act.
- In 1998,best known for was great work and intelligence is Francis Galton. Galton first managed the recorded study of fingerprints.
- In 2010, Simson Garfinkel recognized a topic on facing digital exploration.

OBJECTIVE

The main objectives include here are:

- Designing policy at a suggested misdeed scene that supports you to sure that the digital confirmation acquired is not manipulated.
- It assists to suggest the intention behind the crime and similarity of the main offender.
- It is able to help to retrieve, explores, and maintain computer and acquainted data in such a manner that it favors the inspection agency to represent them as witnessed in a court.
- Retrieving removed files and dispelled documents from digital media to substance the proof and authenticate them.
- This suggests you define the evidence rapidly, and permit you to approximate the potential impression of the malicious action on the victim.

- Generating a computer forensic detail that provides complete details on the exploration process.
- To maintain the evidence following series of custody is needed.

PROCESS OF DIGITAL FORENSICS

The digital forensics operation is a recognized factual and forensics action used in digital forensics inspection. Digital Forensics operation has the following five basic steps:

1. **Identification:** It is the primary phase in a digital forensic activity. The Identification operation largely comprises things such as what proof is present, where it is amassed, and finally how it is gathered (in which arrangement). It identifies prospective sources of applicable evidence as well as key conservator and position of data. Computerized storage media can be personal Mobile phones, computers, PDAs, etc.
2. **Preservation:** It is the operation of preserving relevant computerized stored facts. In this time, data is secluded or isolated. It involves preventing individuals from applying the electronic appliance so that the digital confirmation is not gratified.
3. **Analysis:** At the moment, inspection agents restore particles of data and also draw conclusions established on witness found. Although, it might be taking enough repetitions of examination to assist a special crime thesis. A thoroughly systematic search of proof is connecting to the event being explored.
4. **Documentation:** In this phase, the History of all the detectable data must be designed. Firstly, documents are based on demonstrating technique and methodology. It supports in regenerating the crime scene and evaluating it. It includes proper evidence and documentation of the crime scene along with snapshots and crime-scene retailing.
5. **Presentation:** In this last phase, the operation of outline and summarization and clarification of opinions is done. Digital Forensics not only means simple activity like collect, process, and presents the data. It is all about the current research and also needs to up-to-date, therefore one forensics needs to be a scientist first then after he can be able to join the digital forensics field.

DIGITAL FORENSIC TYPES

Digital forensics is split into specific sub-branches relating to the inspection of various types of evidence.

a. Mobile forensics: It mainly deals with confirmation related to mobile phones and other mobile devices. Most superiorly now a day's mobile phones are the most usual digital evidence found at crime scenes and phones are the most convenient source of evidence.
b. Computer Forensics: It is known as the sub-branch of digital forensics. It mainly operates cases linked to data stored in the computer devices. The goal of computer forensics conflict is to find out and describe the present condition of digital evidence stored into devices like laptops, computers, storage devices, and other electronic devices.
c. Network Forensics: It mainly deals with cases interconnected to computer network policy. This network traffic can be LAN or WAN.
d. Database Forensics: It is also a sub-branch that is connecting the review and inspection of the database and the review and inspection of the database and their metadata.This also handles cars linked to the database.
e. Live Forensics: Most probablyit contends with the examination and survey of cases related to a live scenario. It helps to maintain the confirmation of having any changes.
f. Email Forensics: It deals with the retrieval of emails, as well as deleted emails and contact details.
g. Example uses of it: In recent scenario business associations applied digital forensics in such cases-
    - Problems concerns with compliance.
    - Fake investigations

- Investigation on bankruptcy
- Misuses of internet and email in the workplace
- Investigation of fraud cases
- Industrial issues
- Solution on employees controversy

IMPORTANCE OF FORENSIC KNOWLEDGE

Forensics is so much important for justifying anyone. It plays a significant role in law & justice. It helps to provide proper justice to the victim and also supports to catch and punish criminals or culprits. The knowledge of forensics investigation process, techniques and methods provide advantages to an investigator that entire evidence is correctly gathered and gives to maintain authentication, integrity when legal and technical forensics investigation procedure ignored correctly then following problems arise:

- Demolish the proof of the justice system.
- Proof not being acceptable in court due to authenticity and integrity issues.
- Important and useful evidence being destroyed or compromised.

COMPUTER ROLE IN DIGITAL FORENSICS

The job of PC criminology in wrongdoing is simply going to increment sought after in light of the fact that the requirement for help with recovering data that can be utilized as a proof is getting increasingly hard for law implementation. IT aptitude in law implementation isn't a simple position yet furthermore one that changes the essence of law authorization with method and domination to illuminate examples and have unalloyed repercussions.

COMPUTER FORENSICS TOOL

In the field of computer forensics, various kinds of software tools are used. The persons who are engaged with this profession are known as investigators. The operations need to performed by them included search about the encrypted file. The term is known as "live box" and also other new tools are there for the investigation purpose. That's why they are the best in the industry. Most of the cases the common operations are performed like recover of deleting files, recovery of deleted passwords also recover from raw data. The computer forensics tools give the power to the investigators to process all these data to get the solution and close the case.

DIGITAL FORENSICS CHALLENGES

There are lots of ultimatums that are faced by Digital Forensics. These are following as-

- **High volume and speed:** Problems related to storing, acquiring, and processing a lot of information for forensics intentions have been bringing about issues many times, and also are promoted by availability and extensive marketing of digital information.
- **The detonation of complexity:** Evidence is out of control for a single host. This is spread among various virtual or physical locations, like cloud resources, social networks, personal networks- linked storage units. Because of this, more expertise, time, and tools are required to correctly and completely reconstruct evidence.
- **Arise of ant forensics techniques:** Cautious measures incorporate encryption, jumbling, and shrouding methods, including data stowing away. Collaboration among universal purviews, in any case, researching cybercrime and gathering proof is fundamental in building hermetically sealed cases for law requirement
- **Legitimacy:** Present-day foundations are getting mind-boggling and virtualized, regularly moving their multifaceted nature at the outskirt, (for example, in haze figuring) or designating a few obligations to outsiders, (for example, in stage as-an administration systems).

- **Privacy investigations:** These days, people are spending lots of time with the internet and share various memories of life, essentially through online informal organizations or web-based life destinations. It helps to find and gather all data to make an attack that maltreats a client's security also it linked with various problems when computing is appended.
- **Improvement of standards:** The examinations of front line cybercrimes may require handling data in a cooperative way or utilizing redistributed capacity and calculation. Accordingly, a center advance for the computerized criminology network will be the improvement of appropriate standard arrangements and deliberations.

CONCLUSION

Throughout the discussion, we come to this conclusion that digital forensics is very important to our society and it has become very easier with the help of computers only. Evidence is out of control for a single host. This is spread among various virtual or physical locations, like cloud resources, social networks, personal networks- linked storage units. Because of this, more expertise, time, and tools are required to correctly and completely reconstruct evidence. So the role of computers in digital forensics is very important and useful.

REFERENCES

B.Martini, An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71-80. (2016).

B. Carrier, Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence, 1(4), 1-12. (2016).

M. D.Kohn, M. M.Eloff and J. H. Eloff, Integrated digital forensic process model. Computers & Security, 38, 103-115. (2016).